REMARKS/ARGUMENTS

Applicant acknowledges receipt of the Office Action dated December 20, 2005. Claims 1-8 have been amended with new claims 11-16 being added. Reconsideration and further examination are respectfully requested.

TELEPHONE CONFERENCE

The undersigned wishes to thank the Examiner for the telephone conference dated March 16, 2006. During the telephone conference, claims 1-8 were discussed along with the reference to Williams, Turbo Product Code Tutorial. The Examiner requested that Applicants summarize the use and application of turbo product codes as set forth by Williams in this response. The undersigned discussed that turbo product codes were an advanced form of non-cryptographic encoding, and that the undersigned had uncovered a non-prior art reference that may assist the Examiner in their use and application. The undersigned indicated that he would submit a courtesy copy of this non-prior art reference as an exhibit in this application as an aid to understanding the technology. The Examiner requested that the Applicants review the USPTO Interim Guidelines for Examination of Patent Applications, OG Notice of 22 November 2005. The Examiner further requested that Applicants review the corresponding European patent application for purposes of information disclosure.

Upon review of the subject application file, the corresponding PCT Search Report was filed in this application on June 24, 2002. The PCT Search Report was the only search report filed in the corresponding European Patent Specification EP 1 307 993 B1.

APPENDIX

As a courtesy to the Examiner and to clarify some of the technology in this application, the Applicants submit herewith the following 5 exhibits. Because the following 5 exhibits are clarifying, and hence not material to patentability, no separate Information Disclosure Statement is required.

1. Serge Vaudenay, "On the need for multipermutations ..." cited in the PCT Search Report as category "A" -- general state of the art.

2. Florent Chabard, "On the security of some cryptosystems ..." cited in the PCT Search Report as category "A" -- general state of the art.

3. Anne Canteaut, et al., "A new algorithm for finding minimum-weight words..." cited in the PCT Search Report as category "A" -- general state of the art.

4. David Williams, "Turbo Product Code Tutorial," 1 May 2000, pp. 1-63. This is the full document of the Williams reference discussed in this application.

5. Jessica Pursley, "Turbo Product Codes and Channel Capacity," undated, pp. 1-13. This document clarifies the purpose and application of Turbo Product Codes.

REJECTION UNDER 35 U.S.C. § 103

Claims 1, 3-4, and 7-8 stand rejected under 35 U.S.C. § 103 as being obvious over Rijmen et al., "The Cipher SHARK," Loureiro et al., "Function Hiding Based on Error Correcting Codes," and Williams, "Turbo Product Code Tutorial." The obviousness rejection is respectfully traversed. Claims 2 and 5 stand rejected as obvious over Rijmen et al., Loureiro et al., Williams, and further in view of FOLDOC. All obviousness rejections rely upon Williams.

By way of review, the present invention relates to the art of cryptography. Broadly stated, cryptography relates to the practice of data encryption wherein the security of the system depends upon the secrecy of a key rather than the secrecy of the underlying encryption method. The basic idea is to come up with a method of encryption that resists external attacks. In 1976, the United States selected an encryption methodology, i.e. a cipher, that is known as the Data Encryption Standard ("DES"). The DES provided a combination of confusion (non-linear elements) and diffusion (linear recombination of elements). According to the present invention, "confusion" is provided in FIG. 4 by a plurality of "s-boxes" that are shown in operation 320. Each s-box provides a substitution for the original data according to a look-up table. The "diffusion" is provided by linear transformation operation 330.

One would initially think that a "maximum" amount of diffusion, i.e. a maximum amount of rearrangement of the outputs from the s-boxes in FIG. 4, would be preferred. This is not the case. As set forth in the application at page 2, "maximum" diffusion was suggested by Vaudenay by using Maximum Distance Separable ("MDS") codes. However, the applicants have discovered, as set forth in page 2, ln. 22-27, that maximum diffusion provides a more regular data structure and is therefore more vulnerable to attack.

As now particularly set forth in claim 1, a linear transformation matrix A is created with the processing apparatus by first generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code. This binary [n,k,d] error-correcting code relates to the original information, but also contains some redundant information. Next, some of the redundant information in the binary [n,k,d] code is changed by ***shortening*** the error-correcting code; and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular. The purpose here is simply to "mix up," i.e. diffuse, the original data. Because some of the data in the binary [n,k,d] code is redundant, the code may be shortened without losing the information content.

The reference to Williams, "Turbo Product Code Tutorial" is relied upon as teaching that code shortening enhances flexibility of Turbo Product Codes. As a first matter, turbo product codes are error correcting codes because they contain redundant information. However turbo product codes are primarily used in "noisy" digital communication, such as cellular telephone communication or satellite communication. In those cases, the original information may become corrupted, and the redundant information is then used to reconstruct the data. While turbo product codes are "coded" they are not encrypted. The purpose of the turbo code is to reconstruct the data. This is completely contrary to the purpose of encryption, which is to subvert the reconstruction of the data.

Williams sets forth on page 38 that turbo product codes can be in a wide range of code rates and block sizes. However, the reason is more clearly set forth on page 36 (which is now submitted herewith as EXHIBIT 4), wherein turbo codes are "readily adapted to most any

constellation." In other words, turbo codes are flexible because they can be changed to interface with existing data transmission and reception hardware. Older systems cannot handle large code words. Hence, turbo codes (as opposed to concatenated Reed-Solomon/Viterbi codes) may be shortened in order to be flexible with older systems. In other words, one would not shorten a turbo code of Williams and then extend a matrix B with 2k-n columns such that a resulting matrix C is non-singular, as claimed, because to do so would result in loss of the redundant information. The redundancy in turbo product codes is the very purpose of use according to Williams ("maximize data reliability" at pg. 4 of Williams).

Thus, one skilled in the art would not look to the turbo product codes of Williams in order to increase flexibility in an encryption method. The "shortening" of Williams is for flexibility in hardware systems for forward error correction, and the Williams "shortening" retains the redundant information. In contrast, the presently claimed feature of shortening looses redundant information for the purposes of diffusion during the act of encryption. Accordingly, it is respectfully submitted that Williams may not be combined with Rijmen et al. and Loureiro et al. for want of motivation. Further, it is respectfully submitted that the "code shortening" on page 38 of Williams retains the redundant information and therefore does not loose some of the redundant information through shortening prior to column expansion as claimed.

Reconsideration and withdrawal of the outstanding obviousness rejection is therefore respectfully requested.

Claim 8, and new claims 11-15:

Claim 8 has been amended to be independent, and incorporates the subject matter from claim 1. New dependent claims 11-15 depend from claim 8 and correspond to dependent claims 2-7. Accordingly, claims 8, and 11-15 are non-obvious for the reasons set forth above with regarding to claim 1. Approval, entry, and allowance are respectfully requested.

Claim 16:

New claim 16 corresponds to original claim 1 in combination with claim 3. Claim 16 sets forth determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix (I_k || P_1 C P_2), have a predetermined multi-bit weight; and using P_1 C P_2 as matrix A. This feature is nether taught nor suggested by the prior art. Approval, entry, and allowance are respectfully requested.

CONCLUSION

While we believe that the instant amendment places the application in condition for allowance, should the Examiner have any further comments or suggestions, it is respectfully requested that the Examiner telephone the undersigned attorney in order to expeditiously resolve any outstanding issues.

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Respectfully submitted,
KRAMER & AMADO, P.C.

Terry W. Kramer
Registration No.: 41,541

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314
Phone: 703-519-9801
Fax: 703-519-9802

Date: March 20, 2006

APPENDIX

1. Serge Vaudenay, "On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER," Laboratoire D'Informatique, Ecole Normale Superieure, 16 November 1994 (1994-11-16), pp. 1-12.

2. Florent Chabard, "On the security of some cryptosystems based on error-correcting codes," Laboratoire D'Informatique De L'ens, 1994, pp. 1-9.

3. Anne Canteaut, et al., "A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length 511" Institut National De Recherche En Informatique et en Automatique, 1995, pp. 1-20.

4. David Williams, "Turbo Product Code Tutorial," aha.com, 1 May 2000, pp. 1-63.

5. Jessica Pursley, "Turbo Product Codes and Channel Capacity," Region 3, IEEE Student Paper Competition, undated, pp. 1-13.